

Tenth Annual Industrial Control System Security (ICSS) Workshop

The 10th Industrial Control System Security (ICSS) Workshop will be held on Tuesday, December 10, 2024, in conjunction with the Annual Computer Security Applications Conference (ACSAC). ACSAC will be held in Waikiki, Hawaii.

Call for Papers. Supervisory control and data acquisition (SCADA) and industrial control systems (ICS) monitor and control a wide range of critical industrial and infrastructure processes, such as water treatment, power generation and transmission, oil and gas refining, and manufacturing. Furthermore, the Industrial Internet of Things (IIoT) is rapidly expanding the interconnectivity of ICS environments and introducing many new threats. These environments have been identified as a key target of more generic threats (ransomware, e.g., CL0p), along with more recent tailored nation-state threats targeting electric transmission and distribution systems (e.g., COSMICENERGY).

The essential requirement for high availability in SCADA and industrial control systems, along with the use of resource-constrained computing devices, legacy operating systems, and proprietary software applications, limits the applicability of traditional information security solutions. The goal of this workshop is to explore new techniques that are more effective and efficient at improving the security and resilience of critical control systems in the face of emerging threats. Papers of interest, including (but not limited to) the following subject categories, are solicited:

- IIoT security
- Intrusion detection and prevention for ICS
- Emerging threats to ICS
- Vulnerability analysis and risk management
- Digital forensics for ICS/PLCs
- Techniques for engineering high(er) assurance ICSs
- ICS-oriented cybersecurity education
- Performance evaluation of security methods and tools in control systems
- Innovative ICS/SCADA testbed designs
- Supply chain vulnerabilities and protections
- Modeling and formal verification of ICS security and resilience properties
- Machine learning for ICS

Technical Paper Submissions

Submissions should be 6-10 pages, using the double-column ACM proceedings format (acmart) template available at <https://www.acm.org/publications/taps/word-template-workflow>, with the [sigconf, anonymous] options. Two additional pages can be used for the Appendix. Note that the reviewers are not expected to read the Appendix.

All submissions must be **anonymous**.

The submission website is <https://easychair.org/conferences/?conf=icss240>

Publication

The accepted workshop papers and slides will be published on the ACSAC website with open access. Last year's proceedings are available at <https://www.acsac.org/2024/workshops/icss/>.

Important Date

Submission Deadline:	August 12, 2024
Acceptance Notification:	September 30, 2024
Final Manuscript due:	October 15, 2024
Workshop Date:	December 10, 2024

Further details about the workshop can be found on the workshop website:

<https://www.acsac.org/2024/workshops/icss/>

Contact the workshop organizers at icss240@easychair.org

Organizing Committees

General Co-Chairs:

Harvey Rubinvitz, The MITRE Corporation
Greg Shannon, Idaho National Laboratory

Program Co-Chairs:

Gabriela Ciocarlie, University of Texas at San Antonio/The Cybersecurity Manufacturing Innovation Institute (CyManII)
Ifan Ahmed, Virginia Commonwealth University

Panel Chair

TBD

Proceedings Chair

TBD

Publicity Chair

TBD

Program Committee Members include:

TBD

Workshop Registration

If you are interested in attending, please check off the appropriate box on the conference registration form and add in the Industrial Control System Security (ICSS) Workshop fee.

For accepted papers, at least one author must register and attend.